Hewlett Packard
Enterprise

RWL Tech Note

Comware Routers with L2TP VPN

Prepared by
Richard Litchfield
HPE Networking Solution Architect

Hewlett Packard Enterprise Australia
410 Concord Road
Rhodes NSW 2138
AUSTRALIA

Date Prepared: 24-Aug-17

Document Information

		Document Version No:	1.1
Prepared By:	Richard Litchfield	**Document Version Date:**	24-Aug-17
Reviewed By:		**Review Date:**	

Version History

Ver.	Ver. Date	Revised By	Description	Filename
0.5	7-Jul-17	Richard Litchfield	Initial draft	RWL TechNote – Comware Routers with L2TP VPNv0.5.docx
1.0	12-Jul-17	Richard Litchfield	First release	RWL TechNote – Comware Routers with L2TP VPN v1.0.docx
1.1	24-Aug-17	Richard Litchfield	Using 2 groups	RWL TechNote – Comware Routers with L2TP VPN v1.1.docx

Proprietary Notice

Table of Contents

1. Introduction

1.1. Purpose and Scope

The information provided in this document is designed to assist a suitably skilled practitioner to implement a remote access VPN using L2TP on the Comware routing platforms.

1.2. Sample Configurations

HPE Networking has developed one or more sample configurations to show possible use cases. They are samples only, and do not take into account specific requirements or restrictions that may be present in a customer production environment.

1.3. Definitions and Abbreviations

HPE	Hewlett Packard Enterprise
HPN	HPE Networking
HPGM	HP Global Method (Project Management)
AAA	Authentication, Authorisation, Accounting
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DDNS	Dynamic DNS
DNS	Domain Name System
L2TP	Layer 2 Tunneling Protocol
LNS	L2TP Network Server
MSR	Multi-Service Router (from HPE)
NQA	Network Quality Analyzer
PAP	Password-based Authentication Protocol
POE	Power over Ethernet
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
QOS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
SSH	Secure Shell
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

1.4. Conventions used in this Document

```
CLI switch output.
Specific CLI commands.
Key items to focus on.
```

1.5. Related Documents and References

Version/Date	Author	Document Name
2016	HPE	HPE FlexNetwork MSR Router Series Comware 5 Layer 2 - WAN Access Configuration Guide
2017	HPE	HPE FlexNetwork MSR Router Series Comware 7 Layer 2 - WAN Access Configuration Guide

1.6. Public References

1.6.1. HP Networking

http://www.hpe.com/networking
The HPE Networking starting point!

http://www.hpe.com/networking/support
Manuals, updates, guides, white papers are available for all HP products
Support forums for all HP Networking products

1.6.2. Specific References

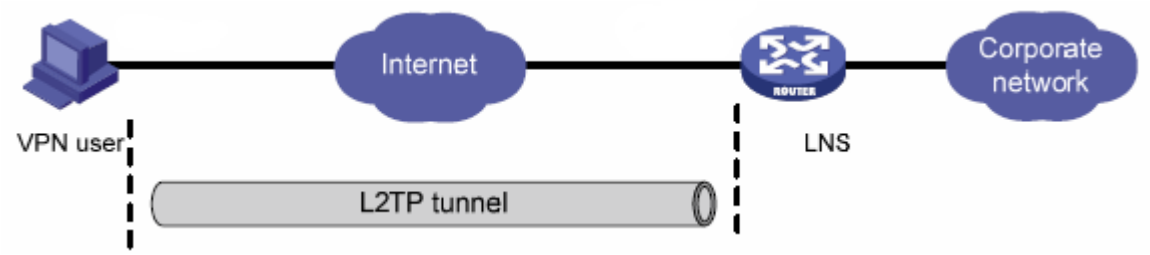
2. Solution Overview

2.1. L2TP

L2TP is a widely used tunneling protocol. L2TP (defined in RFC 2661) is a tunneling protocol that transmits PPP frames. It extends the PPP model by allowing the Layer 2 endpoints that connect to users and PPP endpoints to reside on different devices interconnected by a packet-switched network, such as the Internet.

L2TP by itself does not provide security for connections. However, it has all the security features of PPP and allows for PPP authentication (CHAP or PAP). L2TP can also cooperate with IPsec to guarantee data security, strengthening the resistance of tunneled data to attacks. Tunnel encryption, end-to-end data encryption, and end-to-end application-layer data encryption technologies can be used together with L2TP for higher data security as required.

2.2. Configuration Scenario



The configuration described in this document will allow remote devices to connect to the local network, and receive an IP address on the local network. With no other routing, ACL or firewall restrictions in place, the remote device will have full access to the local network.

2.3. Devices Used

During the preparation of this document, the following devices were used.

2.3.1. MSR930 Router

- Running Comware 5
- Model JG665A

2.3.2. MSR954 Router

- Running Comware 7
- Model JH297A

2.3.3. MSR3012 Router

- Running Comware 7
- Model JG409A

3. Comware 5

All the examples in this section are from the MSR930 running Comware 5.

3.1. Configuration

3.1.1. Local User

Create user accounts as required. Accounts local to the router is the simplest way of doing this, and is ideal for testing and simple remote management functions where only a small number of users are required. Section 6.2 shows how to use RADIUS (ClearPass) for external user authentication.

```
local-user BV-remote                ← create user called BV-remote
 password cipher xxxxxx
 access-limit 2                     ← no more than 2 concurrent logins
 service-type ppp                   ← limited to PPP access


domain system
 authentication ppp local                          ← use local account for PPP access
 ip pool 1 192.168.247.201 192.168.247.247         ← pool for remote user IP addresses
```

3.1.2. L2TP

Enable L2TP and configure the virtual interface.

```
l2tp enable


interface Virtual-Template1
 ppp authentication-mode chap ms-chap-v2 domain system      ← See Section 6.1
 remote address pool 1                                      ← the pool created in the domain
 ip address 192.168.247.1 255.255.255.0                     ← this IP address must be in the same subnet as the pool
```

Create an L2TP group and specify the VT interface for receiving calls.

```
l2tp-group 1
 allow l2tp virtual-template 1
 tunnel name LNS
```

3.2. Connection Testing

```
[MSR930]dis l2tp session
 Total session = 1

 LocalSID  RemoteSID  LocalTID
  23138     1          1
[MSR930]dis l2tp tunnel
 Total tunnel = 1

 LocalTID RemoteTID RemoteAddress    Port   Sessions RemoteName
 1        3         49.181.229.195   12187  1        RWLNB6
```

5. Comware 7

All the examples in this section are from the MSR 954 running Comware 7.

5.1. Configuration

5.1.1. Local User

Create user accounts as required. Accounts local to the router is the simplest way of doing this, and is ideal for testing and simple remote management functions where only a small number of users are required. Section 6.2 shows how to use RADIUS (ClearPass) for external user authentication.

```
local-user remoteuser class network            ← create user called remoteuser
 password cipher xxxxxx
 service-type ppp                              ← limited to PPP access
 authorization-attribute user-role network-operator


domain system
 authentication ppp local                      ← use local account for PPP access
```

5.1.2. Address Pool

Create an IP address pool for PPP.

```
ip pool Remote 10.20.32.2 10.20.32.6           ← IP pool is called "Remote"
ip pool Remote gateway 10.20.32.1              ← gateway IP address also included here
```

5.1.3. L2TP

Enable L2TP and configure the virtual interface.

```
l2tp enable


interface Virtual-Template1
 ppp authentication-mode chap ms-chap-v2 domain system      ← See Section 6.1
 remote address pool Remote                    ← the IP pool created previously (here called "Remote")
```

Create an L2TP group and specify the VT interface for receiving calls.

```
l2tp-group 1 mode lns
 allow l2tp virtual-template 1
 undo tunnel authentication
 tunnel name LNS
```

5.2. Connection Testing

```
 [MSR954]display l2tp ?
  session  L2TP session information
  tunnel   L2TP tunnel information
  va-pool  Virtual access interface pool information
```

6. Security

6.1. PPP Authentication

Multiple options are available to authenticate the PPP connection.

```
[MSR930-Virtual-Template1]ppp authentication-mode ?
  chap        Enable CHAP authentication
  ms-chap     Enable MS-CHAP authentication
  ms-chap-v2  Enable MS-CHAP-V2 authentication
  pap         Enable PAP authentication
```

I have successfully tested PAP, CHAP and MS-CHAP-V2 with Windows clients.

PAP is not recommended because both the username and password are transmitted in clear text.

6.2. RADIUS

RADIUS servers like Microsoft NPS or Aruba ClearPass can be used instead of local authentication. This is a more scalable and flexible way of managing user access.

The commands in this Section are for Comware 5. There are some minor differences with Comware 7.

6.2.1. Configure RADIUS

Create a new scheme for RADIUS.

```
radius scheme clearpass
 server-type extended
 primary authentication 172.20.100.188
 primary accounting 172.20.100.188
 key authentication cipher xxxxxx
 key accounting cipher xxxxxx
 user-name-format without-domain
 nas-ip 172.20.250.254
```

6.2.2. Configure Domain

Create a new domain that uses RADIUS for AAA.

```
domain radius-clearpass
 authentication ppp radius-scheme clearpass      ← use the “clearpass” scheme created in Section 6.2.1
 authorization ppp radius-scheme clearpass
 accounting ppp radius-scheme clearpass          ← without accounting, the login will not complete!
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 ip pool 1 192.168.247.201 192.168.247.247       ← gateway specified in the virtual template Section 6.2.3
```

6.2.3. Virtual Template Interface

Modify the virtual template to replace the local domain with the RADIUS domain.

```
interface Virtual-Template1
 ppp authentication-mode chap ms-chap-v2 domain radius-clearpass
 remote address pool 1
 ip address 192.168.247.1 255.255.255.0
```

6.2.4. ClearPass Configuration

Sample ClearPass Service Profiles are shown in Section

6.3. IPsec

IPsec can be used together with L2TP for higher data security as required.

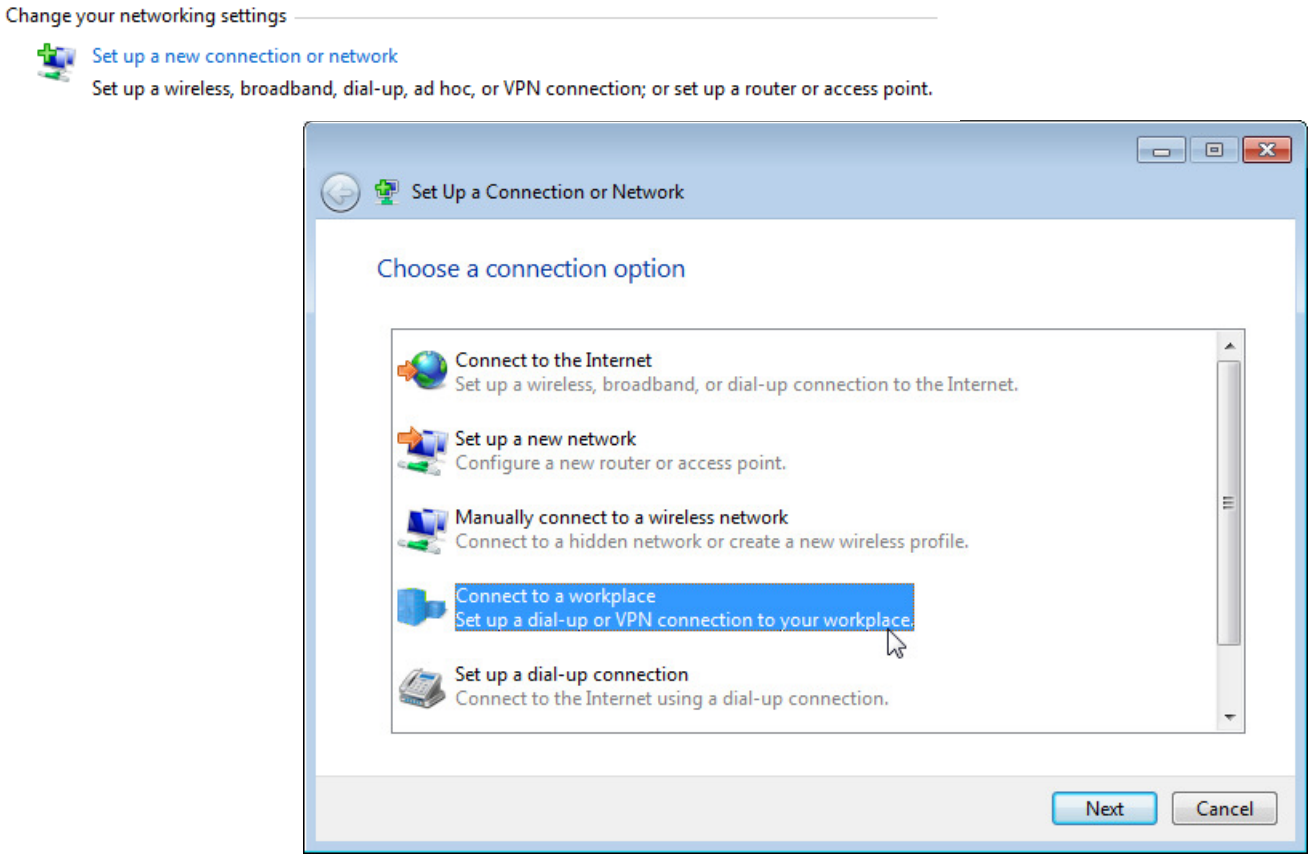
Integration of IPsec and L2TP is not covered in this version of the document.

7. Client Configuration

7.1. MS Windows

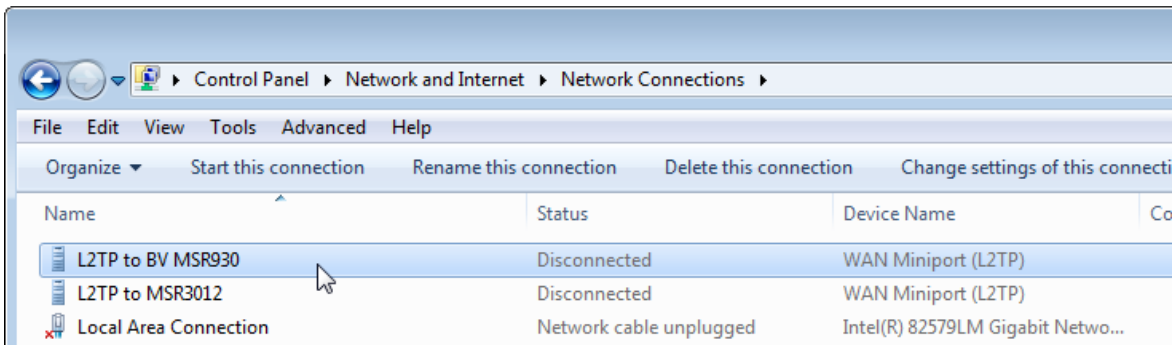
7.1.1. New Network Connection

Create a new network connection. This can be done manually, or with the help of the included wizards.



7.1.2. Configure Network Connection

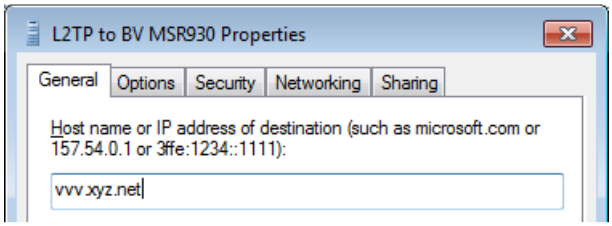
In this example, the new network connection is called *L2TP to BV MSR930*.



Check that the configured options match the site router being connected to, and the client device capabilities.

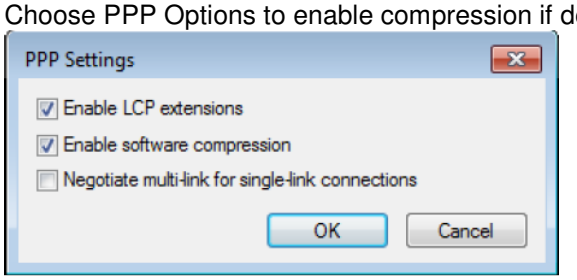
7.1.2.1. General

An IP address or FQDN will work here. I have also used dynamic DNS (DDNS) in the Comware routers to enable use on sites where the IP address is not fixed (very common for the lower-cost, non-SLA ISP offerings).



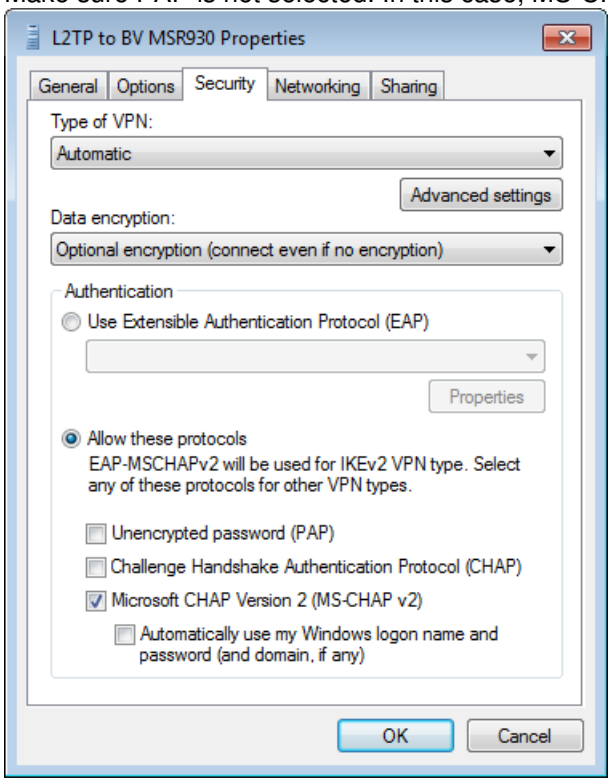
7.1.2.2. Options

Choose PPP Options to enable compression if desired.



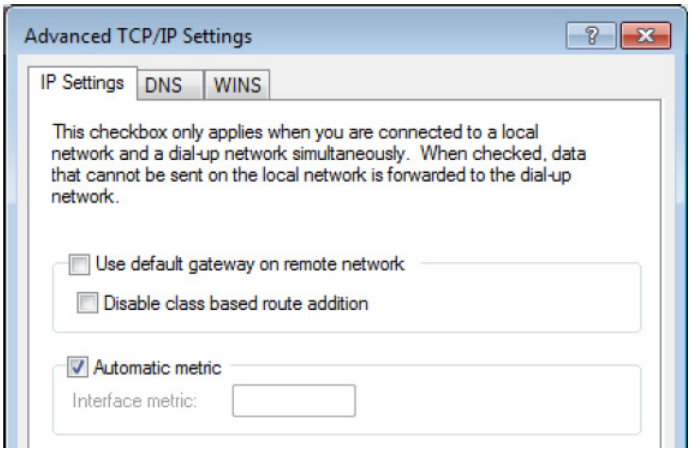
7.1.2.3. Security

Make sure PAP is not selected. In this case, MS-CHAP-V2 is supported at both ends.



7.1.2.4. Networking

From the Networking tab, select TCP/IP V4 and click Properties.
Click on the Advanced tab



You will probably want to disable using the default gateway on the remote network. Add some routes to the client to enable split-tunnel, sending the remote traffic through the L2TP tunnel, and everything else out the local gateway.

7.1.3. DOS Batch File

If you do disable the default gateway on the remote network, a batch file similar to this may be useful to quickly

```
: requires elevation (ie run as administrator)
: changes routes for use with L2TP to BV Lab
: based on Huawei 8372 Dongle with Optus SIM
: local and remote IPs may change - do an IPconfig to confirm IP addresses are correct

route print
pause

: add 10.0.0.0 catch-all route
: route add 10.20.0.0 mask 255.255.0.0 10.20.32.1 metric 10
: add BV Lab 172.20.0.0 catch-all route
route add 172.20.0.0 mask 255.255.0.0 192.168.247.1 metric 30

: change default route for all other traffic (ie internet) if the local default has
   changed
: route change 0.0.0.0 mask 0.0.0.0 220.101.112.1 metric 5

route print
```

add the relevant routes to the local machine to access the remote networks.

8. Appendix A: ClearPass Examples

An example ClearPass Service Profile for L2TP remote VPN access.

8.1. Service Profile

8.1.1. Summary

Configuration » Services » Edit - Remote - L2TP

Services - Remote - L2TP

Summary | Service | Authentication | Roles | Enforcement

Service:

Name:	Remote - L2TP
Description:	VPN access over L2TP
Type:	802.1X Wired - Identity Only
Status:	Enabled
Monitor Mode:	Disabled
More Options:	-

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	Framed-Protocol	EQUALS	PPP (1)
2.	Radius:IETF	NAS-Port-Type	EQUALS	Virtual (5)
3.	Radius:IETF	Service-Type	EQUALS	Framed-User (2)

Authentication:

Authentication Methods:	1. [MSCHAP] 2. [EAP MSCHAPv2]
Authentication Sources:	[Local User Repository]
Strip Username Rules:	-

Roles:

Role Mapping Policy:	-

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	L2TP VPN

8.1.2. Service

Name:	Remote - L2TP
Description:	VPN access over L2TP
Type:	802.1X Wired - Identity Only
Status:	Enabled
Monitor Mode:	Enable to monitor network access without enforcement
More Options:	Authorization Profile Endpoints Accounting Proxy

Service Rule

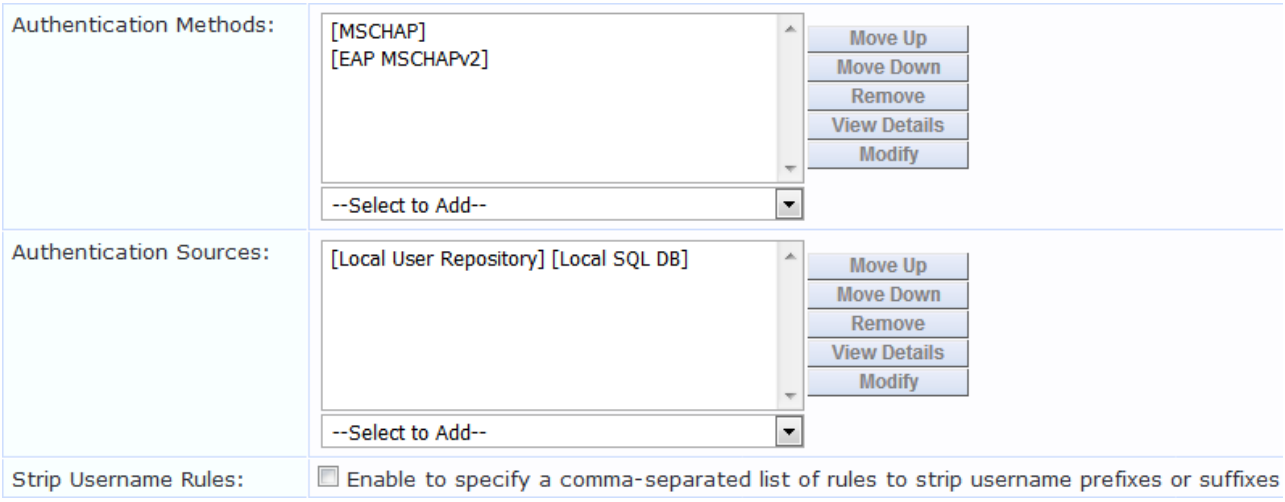
Matches ANY or ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	Framed-Protocol	EQUALS	PPP (1)
2.	Radius:IETF	NAS-Port-Type	EQUALS	Virtual (5)
3.	Radius:IETF	Service-Type	EQUALS	Framed-User (2)

The RADIUS:IETF options that define an L2TP connection are:

- Framed-Protocol = PPP (1)
- NAS-Port-Type = Virtual (5)
- Service-Type = Framed-User (2)

8.1.3. Authentication

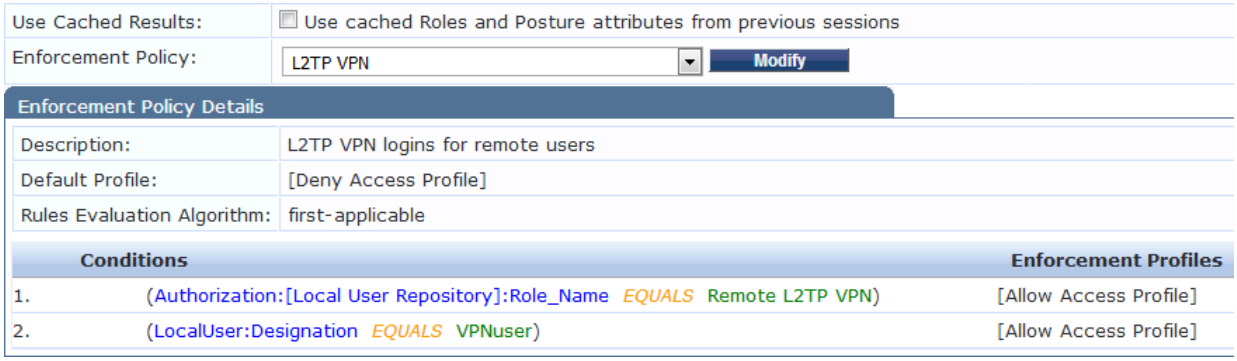


In this case the local ClearPass user database is used; it would be more likely that a joined AD is used as the authentication source.

8.1.4. Roles

Nothing was defined here.

8.1.5. Enforcement

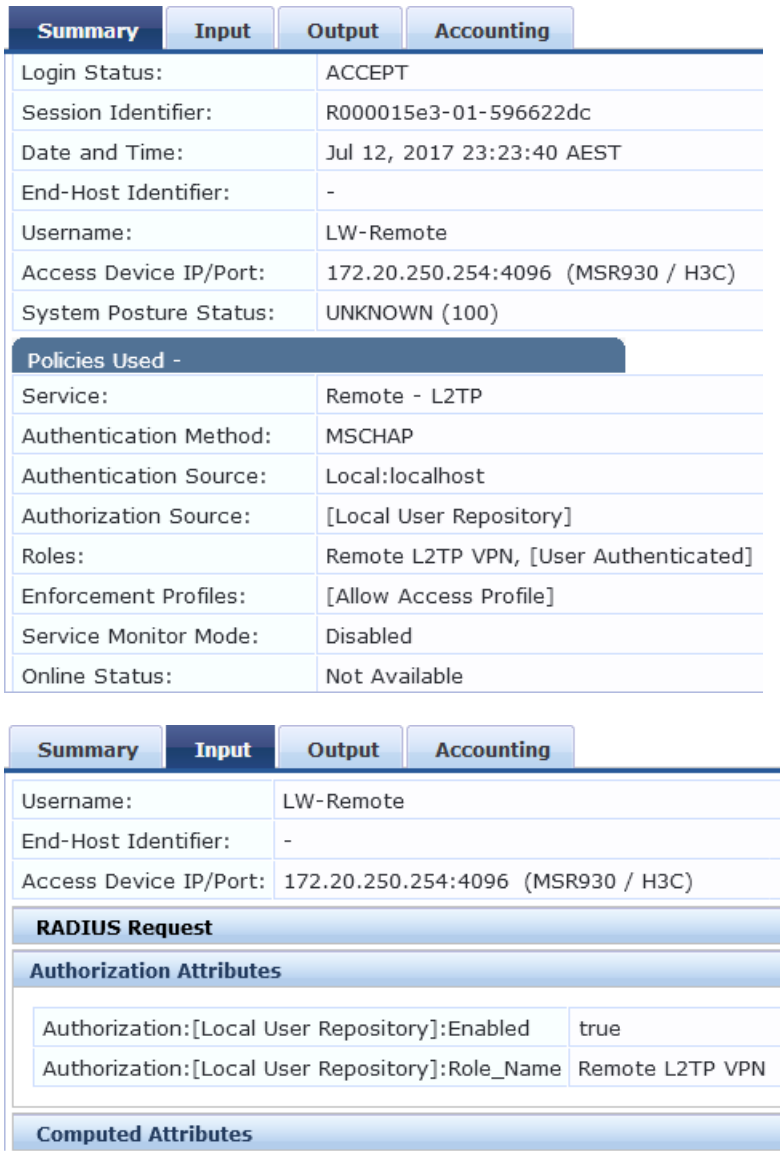


Unless a user is either a member of *Remote L2TP VPN*, or has the designation *VPNuser*, they will be denied access.

8.2. Sample Output

Views from the ClearPass Access Tracker

8.2.1. Login Status: ACCEPT



Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R000015e3-01-596622dc
Date and Time:	Jul 12, 2017 23:23:40 AEST
End-Host Identifier:	-
Username:	LW-Remote
Access Device IP/Port:	172.20.250.254:4096 (MSR930 / H3C)
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	Remote - L2TP
Authentication Method:	MSCHAP
Authentication Source:	Local:localhost
Authorization Source:	[Local User Repository]
Roles:	Remote L2TP VPN, [User Authenticated]
Enforcement Profiles:	[Allow Access Profile]
Service Monitor Mode:	Disabled
Online Status:	Not Available

Summary | Input | Output | Accounting

Username:	LW-Remote
End-Host Identifier:	-
Access Device IP/Port:	172.20.250.254:4096 (MSR930 / H3C)

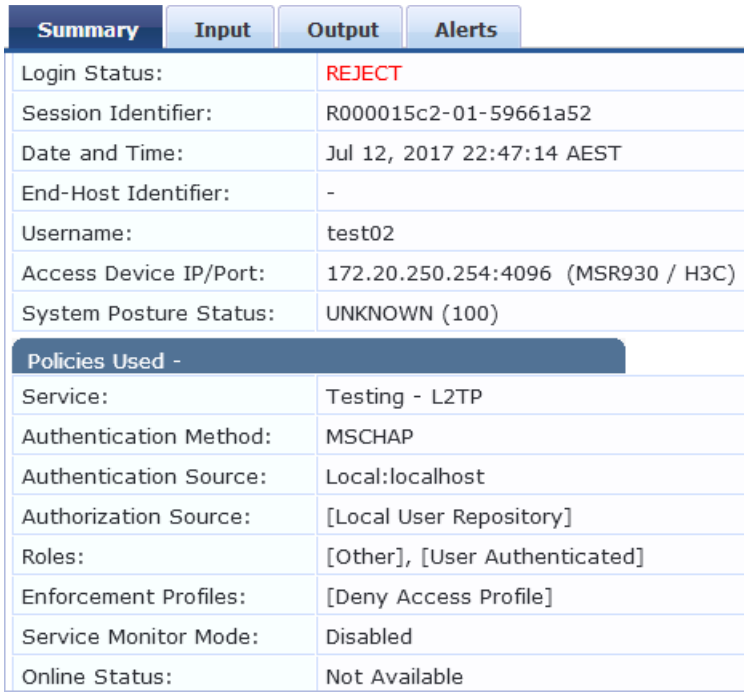
RADIUS Request

Authorization Attributes

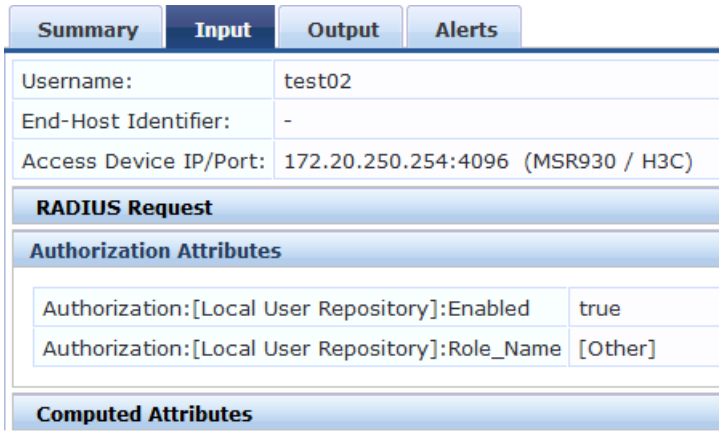
Authorization:[Local User Repository]:Enabled	true
Authorization:[Local User Repository]:Role_Name	Remote L2TP VPN

Computed Attributes

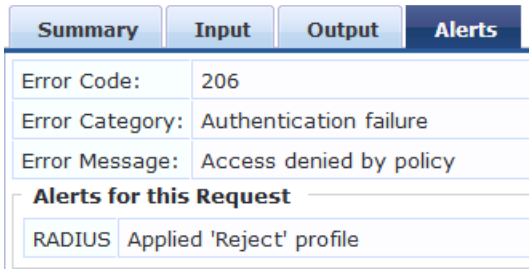
8.2.2. Login Status: REJECT



Summary	Input	Output	Alerts
Login Status:	REJECT		
Session Identifier:	R000015c2-01-59661a52		
Date and Time:	Jul 12, 2017 22:47:14 AEST		
End-Host Identifier:	-		
Username:	test02		
Access Device IP/Port:	172.20.250.254:4096 (MSR930 / H3C)		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Testing - L2TP		
Authentication Method:	MSCHAP		
Authentication Source:	Local:localhost		
Authorization Source:	[Local User Repository]		
Roles:	[Other], [User Authenticated]		
Enforcement Profiles:	[Deny Access Profile]		
Service Monitor Mode:	Disabled		
Online Status:	Not Available		



Summary	Input	Output	Alerts
Username:	test02		
End-Host Identifier:	-		
Access Device IP/Port:	172.20.250.254:4096 (MSR930 / H3C)		
RADIUS Request			
Authorization Attributes			
Authorization:[Local User Repository]:Enabled	true		
Authorization:[Local User Repository]:Role_Name	[Other]		
Computed Attributes			



Summary	Input	Output	Alerts
Error Code:	206		
Error Category:	Authentication failure		
Error Message:	Access denied by policy		
Alerts for this Request			
RADIUS	Applied 'Reject' profile		

9. Appendix B: Sample Configs

These are complete configs for the devices discussed previously.

9.1. Comware 5 on MSR930

```
#
 version 5.20.106, Release 2516P13
#
 sysname MSR930
#
 clock timezone Canberra add 10:00:00
 clock summer-time summer-time repeating 02:00:00 2016 October first Sunday 03:00:00 2017
    April first Sunday  01:00:00
#
 l2tp enable
#
 firewall enable
 firewall default deny
#
 domain default enable system
#
 dns resolve
 dns proxy enable
#
 dar p2p signature-file flash:/p2p_default.mtd
#
 lldp enable
#
 port-security enable
#
 web idle-timeout 20
#
 password-recovery enable
#
acl number 2000
 description NAT OUTBOUND ACL
 rule 10 permit source 10.0.0.0 0.255.255.255
 rule 172 permit source 172.16.0.0 0.15.255.255
#
acl number 3002
 rule 0 permit ip source 172.20.0.0 0.0.255.255 destination 172.25.0.0 0.0.255.255
acl number 3200 name Wan_Inbound
 description WAN_INBOUND_FILTER
 rule 0 permit icmp
 rule 5 remark Allows packets from WGA 172.25 network into BV
 rule 5 permit ip source 172.25.0.0 0.0.255.255
 rule 11 permit udp destination-port eq 1701
 rule 12 permit udp destination-port eq 4500
 rule 15 permit tcp destination-port eq 1723
 rule 25 permit udp destination-port eq 500
 rule 35 permit udp source-port eq 1023
 rule 40 permit gre
 rule 50 permit 50
 rule 51 permit 51
 rule 52 permit udp source-port eq ntp
 rule 53 permit udp source-port eq dns
 rule 54 permit tcp source-port eq domain
 rule 65 remark TCP 25565 is for Minecraft
 rule 65 permit tcp source-port eq 25565 logging
 rule 80 deny udp destination-port eq snmp
 rule 83 deny tcp destination-port eq telnet
```

```
#
vlan 1
#
vlan 250
 description BV MSR DMZ
#
domain system
 authentication ppp local
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 ip pool 1 192.168.247.201 192.168.247.247
#
ike proposal 3
#
ike peer litchwan8
 proposal 3
 pre-shared-key cipher xxxxxx
 id-type name
 remote-name www.xyz.net
 remote-address www.xyz.net dynamic
 local-name vvv.xyz.net
 nat traversal
#
ipsec transform-set litchwan8
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
 esp encryption-algorithm 3des
#
ipsec policy 1048576 2 isakmp
 connection-name litchwan8
 security acl 3002
 ike-peer litchwan8
 transform-set litchwan8
 sa duration traffic-based 1843200
 sa duration time-based 3600
#
dhcp server ip-pool vlan0250 extended
 network ip range 172.20.250.201 172.20.250.249
 network mask 255.255.255.0
 gateway-list 172.20.250.254
 dns-list 8.8.8.8 8.8.4.4
 domain-name dmz.litchwan2.net
 expired day 0 hour 4
#
aspf-policy 1
 detect RTSP
 detect HTTPS
 detect HTTP
 detect SMTP
 detect SSH
 detect FTP
 detect TCP
 detect IKE
 detect UDP
 detect ESP
#
user-group system
 group-attribute allow-guest
#
local-user BV-remote
 password cipher xxxxxx
 access-limit 2
 service-type ppp
```

```
local-user admin
 password cipher xxxxxx
 authorization-attribute level 3
 service-type ssh
 service-type web
#
ssl server-policy access-policy
#
ssl client-policy freedns
 undo server-verify enable
#
cwmp
 undo cwmp enable
#
attack-defense policy 1 interface GigabitEthernet0/0
 signature-detect action drop-packet
 signature-detect fraggle enable
 signature-detect land enable
 signature-detect winnuke enable
 signature-detect tcp-flag enable
 signature-detect icmp-redirect enable
 signature-detect tracert enable
 signature-detect smurf enable
 signature-detect source-route enable
 signature-detect route-record enable
 signature-detect large-icmp enable
 defense scan enable
  defense scan add-to-blacklist
  defense scan blacklist-timeout 30
 defense syn-flood enable
  defense syn-flood action drop-packet
 defense udp-flood enable
  defense udp-flood action drop-packet
 defense icmp-flood enable
  defense icmp-flood action drop-packet
#
ddns policy freedns.afraid.org
 interval 0 0 0
 ssl client policy freedns
 url https://freedns.afraid.org/dynamic/update.php?xxxxxx
#
l2tp-group 1
 allow l2tp virtual-template 1
 tunnel name LNS
#
interface Aux0
 async mode flow
 link-protocol ppp
#
interface Virtual-Template1
 ppp authentication-mode chap ms-chap-v2 domain system
 remote address pool 1
 ip address 192.168.247.1 255.255.255.0
#
interface NULL0
#
interface Vlan-interface1
#
interface Vlan-interface250
 ip address 172.20.250.254 255.255.255.0
 dhcp server apply ip-pool vlan0250
#
interface GigabitEthernet0/0
 port link-mode route
 description Outside - Telstra Cable Modem
 firewall packet-filter name Wan_Inbound inbound
```

```
 firewall aspf 1 outbound
 nat outbound 2000
 ip address dhcp-alloc
 ipsec no-nat-process enable
 ipsec policy 1048576
 attack-defense apply policy 1
 ddns apply policy freedns.afraid.org fqdn vvv.xyz.net
#
interface GigabitEthernet0/1
 port link-mode bridge
 description Inside - BV Lab
 port access vlan 250
#
interface GigabitEthernet0/2
#
interface GigabitEthernet0/3
 port link-mode bridge
 port access vlan 250
#
interface GigabitEthernet0/4
#
interface Cellular-Ethernet0/0
#
interface Cellular-Ethernet1/0
#
ospf 1 router-id 192.168.102.39
 default-route-advertise always
 import-route direct
 area 0.0.0.0
  description BV main routing area
  network 172.20.0.0 0.0.255.255
#
nqa entry imclinktopologypleaseignore ping
 type icmp-echo
  destination ip 172.20.250.253
  frequency 270000
#
 ssl-vpn server-policy access-policy
#
 info-center loghost 172.20.100.185
#
 snmp-agent
 snmp-agent local-engineid 800063A2032C233A119903
 snmp-agent community read public
 snmp-agent community write xxxxxx
 snmp-agent sys-info contact Richard Litchfield
 snmp-agent sys-info location BV Lab
 snmp-agent sys-info version v2c v3
 snmp-agent target-host trap address udp-domain 172.20.100.185 params securityname public
    v2c
 undo snmp-agent trap enable voice dial
#
 header incoming %
Access without authorisation is illegal.
%
 header motd %
Access without authorisation is illegal.
%
#
 dhcp enable
#
 nqa schedule imclinktopologypleaseignore ping start-time now lifetime 630720000
#
 ntp-service unicast-server 216.239.35.4
 ntp-service unicast-server 216.239.35.8
 ntp-service unicast-server 216.239.35.12
```

```
#
 ssh server enable
#
 port-mapping http port 8080
 port-mapping https port 8443
#
 ip https port 8443
 ip https enable
#
 load xml-configuration
#
 load tr069-configuration
#
user-interface aux 0
user-interface vty 0 4
 authentication-mode scheme
 user privilege level 3
 history-command max-size 128
 idle-timeout 30 0
#
return
```

9.2. Comware 7 on MSR954

```
#
 version 7.1.059, Release 0306P12
#
 sysname MSR954
#
 clock timezone EST add 10:00:00
 clock summer-time ESUT 02:00:00 October first Sunday 03:00:00 April first Sunday

01:00:00
#
 router id 192.168.10.254
#
ospf 1
 default-route-advertise always
 area 0.0.0.0
  network 192.168.0.0 0.0.255.255
 area 0.0.0.1
  network 10.1.0.0 0.0.255.255
 area 0.0.0.2
  network 10.2.0.0 0.0.255.255
#
 ip pool Remote 10.20.32.2 10.20.32.6
 ip pool Remote gateway 10.20.32.1
#
 dialer-group 1 rule ip permit
#
 dhcp enable
#
 dns server 8.8.8.8
#
 lldp global enable
#
 password-recovery enable
#
vlan 1
#
vlan 929
 description HPE-Deploy
#
vlan 930
 description Show-Servers
#
dhcp server ip-pool vlan929
 gateway-list 10.20.29.1
 network 10.20.29.0 mask 255.255.255.0
 address range 10.20.29.101 10.20.29.254
 dns-list 8.8.8.8
 domain-name deploy.hpe-aruba.net
 expired day 0 hour 4
#
nqa entry admin 3gkeepalive
 type icmp-echo
  data-size 56
  description General keepalive for LTE link
  destination ip 8.8.8.8
  frequency 180000
#
nqa entry admin testlte
 type icmp-echo
  description Send via LTE
  destination ip 8.8.8.8
  source interface Eth-channel1/0:0
#
```

```
nqa entry imclinktopologypleaseignore ping
 type icmp-echo
  destination ip 10.20.30.254
  frequency 270000
#
 nqa schedule admin 3gkeepalive start-time now lifetime forever
 nqa schedule imclinktopologypleaseignore ping start-time now lifetime 630720000
#
apn-profile telstra.internet
 apn dynamic
#
controller Cellular0/0
 profile main 2
#
controller Cellular1/0
 description LTE with Vodafone SIM
 eth-channel 0
#
interface Virtual-Template1
 ppp authentication-mode chap domain system
 remote address pool Remote
#
interface NULL0
#
interface LoopBack0
 ip address 192.168.10.254 255.255.255.255
#
interface Vlan-interface1
#
interface Vlan-interface929
 ip address 10.20.29.1 255.255.255.0
 dhcp server apply ip-pool vlan929
#
interface Vlan-interface930
 ip address 10.20.30.54 255.255.255.0
#
interface GigabitEthernet0/0
 port link-mode route
#
interface GigabitEthernet0/5
 port link-mode route
#
interface GigabitEthernet0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port trunk pvid vlan 930
 shutdown
#
interface GigabitEthernet0/2
 port link-mode bridge
 description Link to 2920-07
 port access vlan 929
#
interface GigabitEthernet0/3
 port link-mode bridge
 description Link to 3810
 port access vlan 930
#
interface GigabitEthernet0/4
 port link-mode bridge
 description Link to 2920-06
 port access vlan 929
#
interface WLAN-Radio0/0
 shutdown
```

```
#
interface Eth-channel1/0:0
 description Built-in cellular channelised to ethernet
 dialer circular enable
 dialer-group 1
 dialer timer idle 0
 dialer timer autodial 1
 dialer number *99# autodial
 ip address cellular-alloc
 nat outbound 2000
 attack-defense apply policy 1
 apn-profile apply telstra.internet
#
 scheduler logfile size 16
#
line class console
 user-role network-admin
#
line class tty
 user-role network-operator
#
line class vty
 user-role network-operator
#
line con 0
 user-role network-admin
#
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 idle-timeout 45 0
 history-command max-size 128
#
 ip route-static 0.0.0.0 0 Eth-channel1/0:0 description LTE connection
 ip route-static 10.2.0.0 16 10.20.30.1 description HP SSC network
 ip route-static 10.20.0.0 16 10.20.30.1 description HP Roadshow network
 ip route-static 172.16.0.0 12 10.20.30.1 description SSC Cloud and RWL networks
#
 snmp-agent
 snmp-agent local-engineid 800063A2802C233A861D3000000001
 snmp-agent community write xxxxxx
 snmp-agent community read public
 snmp-agent sys-info contact Richard Litchfield
 snmp-agent sys-info location HPE Aruba Roadshow
 snmp-agent sys-info version v2c v3
#
 ssh server enable
#
 ntp-service enable
 ntp-service source Eth-channel1/0:0
 ntp-service unicast-server au.pool.ntp.org
#
acl basic 2000
 description NAT OUTBOUND ACL
 rule 5 permit
#
domain system
 authentication ppp local
#
 domain default enable system
#
role name level-0
 description Predefined level-0 role
#
role name level-1
```

```
 description Predefined level-1 role
#
role name level-2
 description Predefined level-2 role
#
role name level-3
 description Predefined level-3 role
#
role name level-4
 description Predefined level-4 role
#
role name level-5
 description Predefined level-5 role
#
role name level-6
 description Predefined level-6 role
#
role name level-7
 description Predefined level-7 role
#
role name level-8
 description Predefined level-8 role
#
role name level-9
 description Predefined level-9 role
#
role name level-10
 description Predefined level-10 role
#
role name level-11
 description Predefined level-11 role
#
role name level-12
 description Predefined level-12 role
#
role name level-13
 description Predefined level-13 role
#
role name level-14
 description Predefined level-14 role
#
user-group system
#
local-user admin class manage
 password hash xxxxxx
 service-type ssh telnet http
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
local-user remoteuser class network
 password cipher xxxxxx
 service-type ppp
 authorization-attribute user-role network-operator
#
l2tp-group 1 mode lns
 allow l2tp virtual-template 1
 undo tunnel authentication
 tunnel name LNS
#
 l2tp enable
#
attack-defense policy 1
 syn-flood detect non-specific
 syn-flood action drop
 rst-flood detect non-specific
 rst-flood action drop
```

```
 fin-flood detect non-specific
 fin-flood action drop
 udp-flood detect non-specific
 udp-flood action drop
 icmp-flood detect non-specific
 icmp-flood action drop
 signature detect impossible action drop
 signature detect teardrop action drop
 signature detect tiny-fragment action drop
 signature detect ip-option-abnormal action drop
 signature detect smurf action drop
 signature detect ping-of-death action drop
 signature detect tcp-invalid-flags action drop
 signature detect winnuke action drop
 signature detect udp-bomb action drop
 signature detect snork action drop
 signature detect fraggle action drop
#
return
```

10. Appendix C: Troubleshooting

10.1. Connection fails after Authentication

10.1.1. Symptoms

Attempting to log in with an appropriate account appears to work, but the connection does not complete. An additional login screen appears

- ClearPass shows a successful authentication in Access Tracker
- Router shows initial success in debug
- Windows VPN login doesn't fail, but brings up an account window

Only the admin account completed the VPN connection

10.1.2. Troubleshooting

10.1.2.1. ClearPass

- Nothing mismatched or out of the ordinary
- All tested users in the ClearPass local database had exactly the same settings
- Changing username and/or password made no difference unless the username was changed to *admin* or *BV-remote*
- These were the only two user-local accounts on the router

10.1.2.2. Router Debug

Enabled monitor and debug modes on the router, and debugging l2tp.

```
<MSR930>terminal monitor
Info: Current terminal monitor is on.

<MSR930>terminal debugging
Info: Current terminal debugging is on.

<MSR930>debugging l2tp ?
  all         All debugging functions
  control     Control packet debugging functions
  dump        PPP packet debugging functions
  error       Error debugging functions
  event       Event debugging functions
  hidden      Hidden AVP debugging functions
  payload     L2TP data packet debugging functions
  timestamp   Time stamp debugging functions
```

Sample lines from debug showing errors:

```
*Jul 10 23:23:46:338 2017 MSR930 L2TP/7/L2TDBG:  L2TP_ERROR: Found invalid AVP in received
   ICRQ
*Jul 10 23:23:46:786 2017 MSR930 L2TP/7/L2TDBG:  L2TP_ERROR: Packet forwarding failed
   because call 23505 was not established
```

Debugging the PPP authentication process was also useful.
<MSR930>debugging ppp chap all

```
*Jul 11 09:25:50:502 2017 MSR930 PPP/7/debug2:
  PPP Event:
      Virtual-Template1:0 CHAP AAA Result Event
      state WaitingAAA
*Jul 11 09:25:50:502 2017 MSR930 PPP/7/debug2:
  PPP Error:
      Virtual-Template1:0 CHAP : Server authentication failed No.  3 !
*Jul 11 09:25:50:503 2017 MSR930 PPP/7/debug2:
  PPP State Change:
      Virtual-Template1:0 CHAP : WaitingAAA --> ServerFailed
*Jul 11 09:25:50:504 2017 MSR930 PPP/7/debug2:
  PPP Packet:
      Virtual-Template1:0 Output CHAP(c223) Pkt, Len 84
      State ServerFailed, code FAILURE(04), id 3, len 80
      Message: E=691 R=1 C=820caa9d85fe81f0f604ae911fdbd145 V=3 M=Illegal user or password.
*Jul 11 09:25:50:505 2017 MSR930 PPP/7/debug2:
  PPP State Change:
      Virtual-Template1:0 CHAP : ServerFailed --> SendChallenge
```

10.1.2.3. Findings

If RADIUS accounting is *not* enabled, an authenticated user must also match a local user. (Just the name must match; nothing else is checked.) If the case-sensitive user-local name does not match, the VPN connection will not complete.

For example, the two users *admin* and *BV-remote* will connect successfully because they have a local-user account:

```
local-user BV-remote
 password cipher xxxxxx
 access-limit 2
 service-type ppp
local-user admin
 password cipher xxxxxx
 authorization-attribute level 3
 service-type ssh
 service-type web
```

Even without service-type ppp for local-user admin, the connection still completes.

10.1.3. Resolution

Modify the domain for RADIUS to include accounting (and authorisation).

```
[MSR930-isp-radius-clearpass]authorization ppp radius-scheme clearpass
[MSR930-isp-radius-clearpass]accounting ppp radius-scheme clearpass

*Jul 11 09:26:28:886 2017 MSR930 PPP/7/debug2:
  PPP Event:
      Virtual-Template1:0 CHAP AAA Result Event
      state WaitingAAA
*Jul 11 09:26:28:887 2017 MSR930 PPP/7/debug2:
  PPP State Change:
      Virtual-Template1:0 CHAP : WaitingAAA --> ServerSuccess
*Jul 11 09:26:28:887 2017 MSR930 PPP/7/debug2:
  PPP Packet:
      Virtual-Template1:0 Output CHAP(c223) Pkt, Len 71
      State ServerSuccess, code SUCCESS(03), id 4, len 67
      Message: S=A9BC8D98171F7E80A32F4286DFC30314CA78B316 M=Welcome to MSR930.
%Jul 11 09:26:29:049 2017 MSR930 IFNET/5/PROTOCOL_UPDOWN: Protocol PPP IPCP on the
interface Virtual-Template1:0 is UP.
```

If you are using ClearPass as your RADIUS server, you will also now see an additional Accounting tab when looking at successfully connected users in the Access Tracker.

11. Appendix D: Additional Use Cases

11.1. Two Groups/IP Pools

11.1.1. Requirement/Problem Statement

Client initiated L2TP tunnel is working with a single IP, but a second pool is required. However, for L2TP groups other than 1, the remote remote-name option must also be configured. Without the remote name, additional groups cannot be configured.

11.1.2. Observations and Changes

These are based on the MSR930 running Comware 5, and the sample config in Section 9.1.

Running this command shows the remotename that needs to be added into the group 2 config.

```
[MSR930]dis l2tp tunnel
Total tunnel = 1

LocalTID RemoteTID RemoteAddress  Port  Sessions RemoteName
1        1         49.181.174.182 48496 1        RWLNB6
```

These additional lines were added to enabled a second group with a different IP subnet (192.168.248.0/24).

```
#
l2tp-group 2
allow l2tp virtual-template 2 remote RWLNB6
tunnel name LNS2
tunnel avp-hidden
#
interface Virtual-Template2
ppp authentication-mode chap ms-chap-v2 domain radius-clearpass
remote address pool 2
ip address 192.168.248.1 255.255.255.0
#
domain radius-clearpass
ip pool 2 192.168.248.201 192.168.248.247
#
```

11.1.3. Testing

Before adding the lines above to the config, the device connecting through the T2TP tunnel received an IP address in the 192.168.247.0/24 range (see figure in Section 10.1.3). After adding the second group to the config, the device connecting through the T2TP tunnel received an IP address from the new 192.168.248.0/24 range. This is shown in the ClearPass Access Tracker log as the “framed IP address”: